

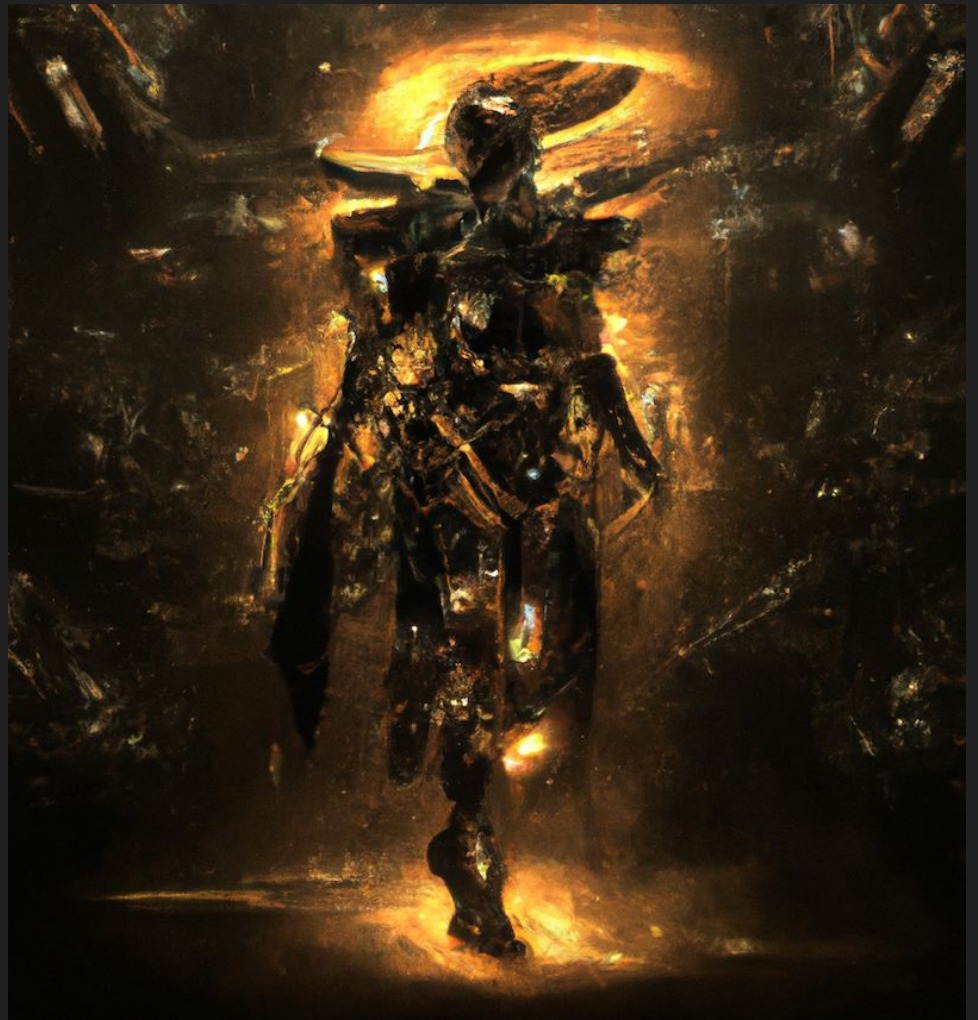
Influence operation 101 example

By

Jindrich Karasek aka **4n6strider**



TLP:Amber



What: (In theory)



incl. economic warfare and
military operations, etc.

e.g., influence operations

Hybrid
warfare

Cognitive
warfare

Information
warfare

Cyber-
warfare

e.g., brain control

e.g., media control

practical attacks on infrastructure
(e.g., DDoS attacks).



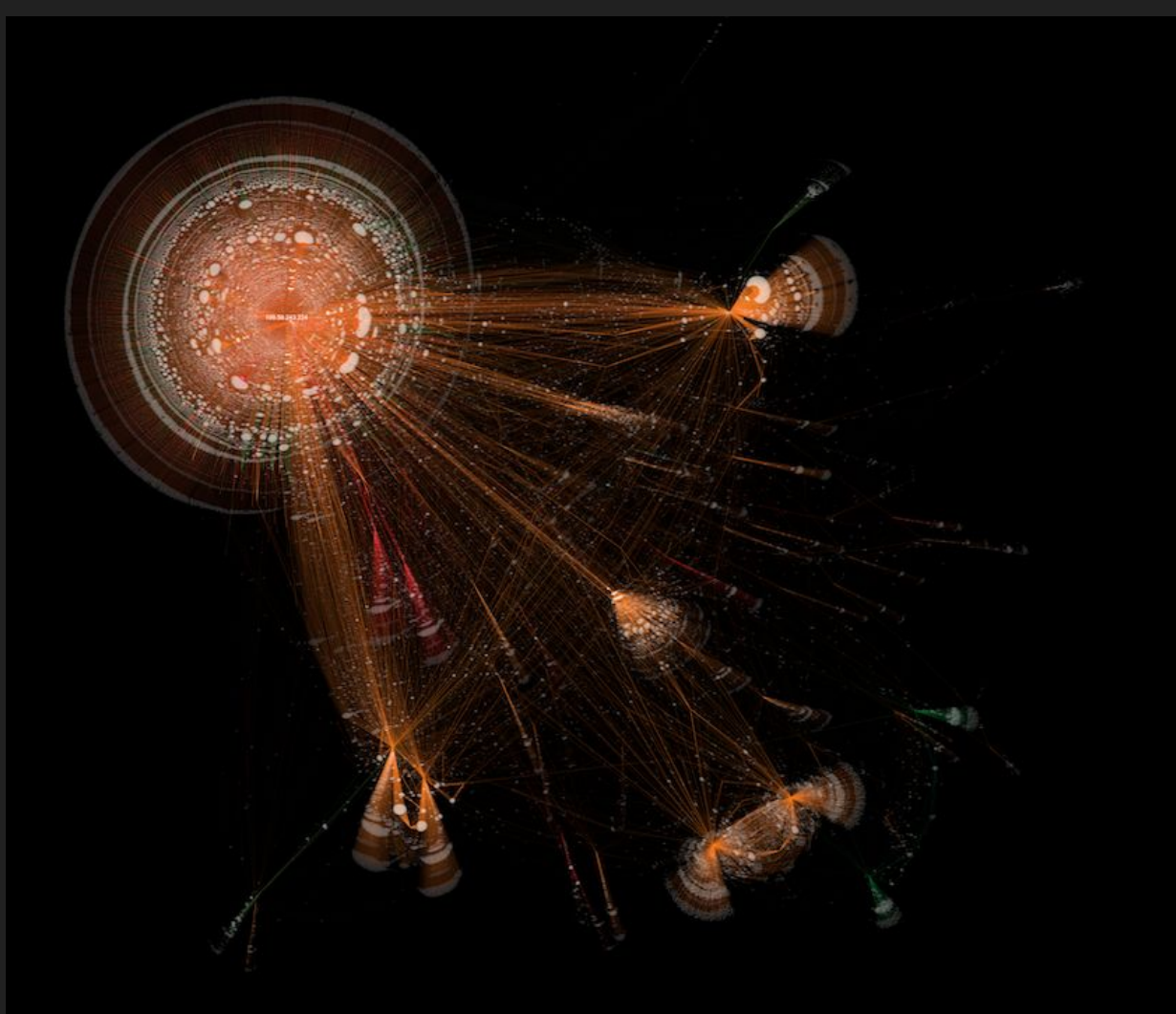
TLP:Amber

Dataset:

- 750 distinct URLs
- 430 domains
- 128 IPs
- 448 259 netflows
- 498 760 pDNS records
- Processed with **Eolas**

<https://github.com/Eolas-bith/UNICRI-De-code-CW>

TLP:Amber




```
https://connect.facebook.net/signals/config/765819157890167?v=2.9.125&r=stable&domain=news.ceska.kantaapnews.comhttps://connect.facebo
ok.net/en_US/fbevents.js
!function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)n=
n._fbq=n;n.push=n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;
t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','https://connect.facebook.net/en_US/fbevents.js');
fbq('init', '90167');
fbq('track', 'AddToCart');
```

https://news.ceska.kantaapnews.com/lander/Fd

Novinky.cz » Politika » První zákon Petra Pavla o zajištění finančního zabezpečení občanů – přijat

První zákon Petra Pavla o zajištění finančního zabezpečení občanů – přijat

pondělí 28. srpna 2023 – Praha
[Lukáš Zaccpal](#)



KryspinGroup Trade Platform

Úroveň marže 0% Použitá marže: 0 Kapitál: \$0.00 Balance: \$0.00 Naser Teei Usau VKLAD
Dostupné marže: \$0.00 P/L: \$0.00 Kredit: \$0.00 15cm@gmail.com

Hledat Všechny BTC/USD 5m GOOG 5m AAPL 5m TSLA 5m _BMW.DE 5m

Active Prodejní certifikákní cena

AUD/CHF	0.56796	0.56823
AUD/JPY	94.157	94.178
AUD/NZD	1.08712	1.08748
AUD/USD	0.64235	0.64246
CAD/CHF	0.65127	0.65158
CAD/JPY	107.976	107.976
CHF/HUF	400.75	401.38
CHF/JPY	165.747	165.772
EUR/AUD	1.68248	1.68272
EUR/CAD	1.46715	1.46748
EUR/CHF	0.95575	0.95597
EUR/DKK	7.4519	7.4534
EUR/GBP	0.85902	0.85917
EUR/HUF	383.15	383.37
EUR/ILS	4.1045	4.1045
EUR/JPY	158.496	158.494

_BMW.DE - 5 096.640 H96.640 L96.620 C96.620 -0.030 (-0.03%)

Objem 1

Investice \$1 045.77
Cena položky 1.08
Ramenec 1:10
Rozšíření 0 pips
Swap Buy -2.81
Swap Sell -2.81
Minimální krok 0.01

SELL 96.62 BUY 96.76

Take profit 0 \$
Stop loss 0 \$

Otevírací pozice (0) Čekající pozice (0) Uzavřené pozice (0)

Symbol Počáteční cena Aktuální kurz Take Profit Stop Loss Výměna Zisk \$

V tabulce nejsou k dispozici žádné údaje

ČESKÉ ELEKTRÁRNY SPOUŠTĚJÍ PROGRAM PODPORY OBČANŮ

first_name is required

Jméno

last_name is required

Příjmení

email is required

Tvůj e-mails

phone must be a valid phone number

+420 + 601123 456

Poslat zprávu



Snažili jsme se, aby náš produkt byl jedinečný a užitečný.

```

<!DOCTYPE html>
<html lang=
  ><head> </head>
  ><body id="body">
    ><header class="page-header"> </header>
    ><main class="page-main">
      ><section class="page-start page-section">
        ><div class="container">
          ><h1 class="page-title"
            text-white text-center"> </h1>
          ><div class="row align-items-center
            justify-content-between flex-md-row-reverse pt
          ><div class="col-12 col-md-6 col-lg-5 mb-2 ">
            ><div class="page-form" id="page-form">
              ><form action="thankyou.php" method="POST" class="page-form_
                <input name="__form_id" type="hidden" value="1">
                ><div class="page-form_group focus"> </div>
                ><div class="page-form_group focus"> </div>
                ><div class="page-form_group focus"> </div>
                ><div class="page-form_group"> </div>
                ><button type="submit" class="page-form_btn page-btn"> Poslat zprávu </button>
                <input type="hidden" name="flow_hash" value="64c114005b6be06074">
                <input type="hidden" name="landing" value="Cez Group">
                <input type="hidden" name="facebook_pixel_id" value="{facebook
                <input type="hidden" name="click_id" value="{subid}">
                <input type="hidden" name="sub1" value="{sub1}">
                <input type="hidden" name="sub2" value="{sub2}">
                <input type="hidden" name="sub3" value="{sub3}">
                <input type="hidden" name="sub4" value="{sub4}">
                <input type="hidden" name="landing_url" value="https://gosla
              </form>
            </div>
          </div>
        </div>
        ><div class="col-12 col-md-6 col-lg-7"> </div>
      </div>
    </section>
    ><section class="features"> </section>
    ><section class="about"> </section>
  </main>
  ><footer class="page-footer"> </footer>
  ><div class="modal" id="privacy" tabindex="-1" aria-labelledby="exampleModalLabel" aria-hidden="true"> </div>
  <script type="text/javascript" src="https://posthog.gclab.ru/static/recorder.js?v=1.53.3"></script>
  <script defer src="assets/errors-modal/js/errors-modal.js"></script>
  <script defer src="js/bundle.741f2dd...js"></script>
  <script src="js/landing_url2.js"></script>
</body>
</html>

```

(kali@kali)-[~]
 \$ wafw00f goslakinvest.pro



~ WAFW00F : v2.2.0 ~

The Web Application Firewall Fingerprinting Toolkit

```

[*] Checking https://goslakinvest.pro
[+] The site https://goslakinvest.pro is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

```

(kali@kali)-[~]

```

$ sudo nmap -sS -p- -Pn gclab.ru
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 14:01 UTC
Nmap scan report for gclab.ru (31.10.5.10)
Host is up (0.022s latency).
rDNS record for 31.10.5.10: srv17401.hosted-by-eurohoster.org
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1194/tcp   closed openvpn
5001/tcp   closed complex-link
19000/tcp  open  igrid
19001/tcp  closed unknown

```

TLP:Amber

Thank you!

Jindrich Karasek aka 4n6strider
Senior Cyber Threat Researcher at Trend Micro



Version: cd56e0d82428db36a6148644ef7a2ae3592512d0



<https://linktr.ee/4n6strider>

